



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

h

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,357	03/31/2004	Donald A. Zick	14066.0004	5014
<div>7590 01/15/2008</div> <div>Stuart T. F. Huang Steptoe & Johnson 1330 Connecticut Avenue, NW. BOX PTO Washington, DC 20036</div> <div>EXAMINER TOLENTINO, RODERICK</div> <div>ART UNIT PAPER NUMBER</div> <div>2134</div> <div>MAIL DATE DELIVERY MODE</div> <div>01/15/2008 PAPER</div>				

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/813,357

Applicant(s)

ZICK, DONALD A.

Examiner

Roderick Tolentino

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 October 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 10/29/07.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 30 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/29/2007 has been entered.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 5, 11, 15, 21 and 25 have been considered but are moot in view of the new ground(s) of rejection, as necessitated by amendment made by applicant on 10/29/2007.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1 – 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al U.S. Patent No. (6,766,453) in view of Berman et al. U.S. PG-Publication No. (2003/022116), Dujari et al. U.S. Patent No. (7,191,467) and Lintulampi U.S. Patent No. (6,377,804).

6. As per claim 1, Nessett teaches generating a first secret known to the first device and a second secret known to the second device using communications between the first device and the second device over a first communication channel, said first and second secrets ostensibly being the same, (Nessett, Col. 2 Lines 58 – 67) from the first device, producing first information derived from the first secret (Nessett, Col. 2 Lines 58 – 67), from the second device, producing second information derived from the second secret; (Nessett, Col. 3 Lines 1 – 17) but fails to teach using a communication channel other than the first communication channel and a communication method other than the first communication method, comparing the first information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same; and enabling the first and second device to use the first and second secrets upon the third party being assured that the first secret and the second secret are the same and initiating communication between the first device and the second device over a first communication channel using a first communication method by engaging a trigger at the first device and. However, in an analogous art Berman teaches using a communication channel other than the first communication channel and a communication method other than the first communication method, comparing the first

Art Unit: 2134

information and the second information in a manner sufficient to assure a third party that the first secret and the second secret are the same (Berman, Paragraph 0062, communication between server and the authenticating server, which in turn authenticates the user and the server) and Dujari teaches enabling the first and second device to use the first and second secrets upon the third party being assured that the first secret and the second secret are the same (Dujari, Col. 12 Lines 58 – 62, out of band authentication) and Lintulampi teaches initiating communication between the first device and the second device over a first communication channel using a first communication method by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged (Lintulampi, Col. 1 Lines 66 – 67 and Col. 2 Lines 1 – 10, device registers with second device that connects to a network).

At the time the invention was made it would have been obvious to a person of ordinary skill in the art to use, Berman's mutual authentication with secure transport and client authentication with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of secure authentication (Berman, Paragraph 0008).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, Dujari's method of integrating third party authentication with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of being a secure form of authenticating information (Dujari, Col. 22 Lines 10 – 14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, Lintulampi's mobile communication system with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of providing services based on geographic locations (Lintulampi, Col. 1 Lines 4 – 11).

7. As per claims 2, 12 and 22, Nessel teaches the first device and the second device generate the first and second secrets using a Diffie-Hellman key exchange (Nessel, Col. 2 Lines 40 – 57).

8. As per claims 3, 13 and 23, Nessel teaches the first information is derived from a hash of the first secret; and the second information is derived from a hash of the second secret (Nessel, Col. 7 Lines 18 – 27).

9. As per claims 4, 10, 14, 20, 24 and 30, Nessel teaches the first information comprises a credential (Nessel, Col. 2 Lines 61 – 63).

10. As per claim 5, Nessel teaches communicating a commitment from the first device to the second device over a first communication channel, said commitment comprising information derived from a security value known to the first device (Nessel, Col. 6 Lines 49 – 65), communicating from the second device to the first device over the first communication channel, information for use in generating a first secret, communicating the security value from the first device to the second device, generating the first secret at the first device and a second secret at the second device (Nessel, Col. 2 Lines 58 – 67), said first and second secrets ostensibly being the same from the first device, on a communication channel other than the first communication channel, validating first verification information related to the first secret from the second device

Art Unit: 2134

(Nessett, Col. 3 Lines 1 – 17) but fails to teach from the first device, on a communication channel other than the first communication channel and using a communication method other than the first communication method, validating first verification information related to the first secret, from the second device, on a communication channel other than the first communication channel and using a communication method other than the first communication method, validating second verification information related to the second secret and enabling the first and second devices to use the first and second secrets upon a third party being assured that the first secret and the second secret are the same and initiating communication between the first device and the second device over a first communication channel using a first communication method by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged. However in an analogous art Berman teaches from the first device, on a communication channel other than the first communication channel and using a communication method other than the first communication method, validating first verification information related to the first secret, from the second device, on a communication channel other than the first communication channel and using a communication method other than the first communication method, validating second verification information related to the second secret (Berman, Paragraph 0062, another communication system used to verify information, communication between server and the authenticating server, which in turn authenticates the user and the server) and Dujari teaches enabling the first and second devices to use the first and second secrets upon a third party being assured that the

Art Unit: 2134

first secret and the second secret are the same (Dujari, Col. 12 Lines 58 – 62, out of band authentication) and Lintulampi teaches initiating communication between the first device and the second device over a first communication channel using a first communication method by engaging a trigger at the first device and detecting at the second device that the trigger at the first device has been engaged (Lintulampi, Col. 1 Lines 66 – 67 and Col. 2 Lines 1 – 10, device registers with second device that connects to a network).

At the time the invention was made it would have been obvious to a person of ordinary skill in the art to use, Berman's mutual authentication with secure transport and client authentication with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of secure authentication (Berman, Paragraph 0008).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, Dujari's method of integrating third party authentication with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of being a secure form of authenticating information (Dujari, Col. 22 Lines 10 – 14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, Lintulampi's mobile communication system with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of providing services based on geographic locations (Lintulampi, Col. 1 Lines 4 – 11).

11. As per claims 6, 16 and 26, Nessel teaches the commitment is a hash of the security value (Nessel, Col. 7 Lines 18 – 27).

Art Unit: 2134

12. As per claims 7, 17 and 27, Nessett teaches the first verification information is a hash value derived from the first secret and the security value (Nessett, Col. 7 Lines 18 – 27).

13. As per claims 8, 18 and 28, Nessett teaches the first verification information is a hash value derived from a catenation of the first secret with the security value (Nessett, Col. 7 Lines 23 – 27).

14. As per claim 9, 19 and 29, Nessett teaches the length of the verification information is shorter than a length needed to provide a substantially identical level of security in a substantially identical method that does not utilize said commitment (Nessett, Col. 7 Lines 18 – 26, Hashed).

15. As per claims 11, 15 and 21, Nessett disclose generates a first secret that is ostensibly shared with the other device using the first communication channel (Nessett, Col. 2 Lines 58 – 67), but fails to teach an interface to a first communication channel associated with a first communication method, an interface to a second communication channel associated with a communication method other than the first communication method and validates on the second communication channel verification information derived from the ostensibly shared secret, and is enabled to use the ostensibly shared secret upon receipt of an indication that a third party is assured that the first secret is shared with the other device and a trigger coupled to the device, the trigger comprising a switch or a button and a registration process that initiates communication with the other device over the first communication channel upon engagement of the trigger coupled to the device. However, in an analogous art Berman teaches an interface to a

Art Unit: 2134

first communication channel associated with a first communication method, an interface to a second communication channel associated with a communication method other than the first communication method (Berman, Paragraph 0062, another communication system used to verify information, communication between server and the authenticating server, which in turn authenticates the user and the server) and Dujari teaches teach validates on the second communication channel verification information derived from the ostensibly shared secret, and is enabled to use the ostensibly shared secret upon receipt of an indication that a third party is assured that the first secret is shared with the other device (Dujari, Col. 12 Lines 59 – 64) and Lintulampi a trigger coupled to the device, the trigger comprising a switch or a button (Lintulampi, Col. 1 Lines 66 – 67 and Col. 2 Lines 1 – 10, device is a telephone) and a registration process that initiates communication with the other device over the first communication channel upon engagement of the trigger coupled to the device (Lintulampi, Col. 1 Lines 66 – 67 and Col. 2 Lines 1 – 10, device registers with second device that connects to a network).

At the time the invention was made it would have been obvious to a person of ordinary skill in the art to use, Berman's mutual authentication with secure transport and client authentication with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of secure authentication (Berman, Paragraph 0008).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, Dujari's method of integrating third party authentication with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the

Art Unit: 2134

advantage of being a secure form of authenticating information (Dujari, Col. 22 Lines 10 – 14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, Lintulampi's mobile communication system with Nesset's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of providing services based on geographic locations (Lintulampi, Col. 1 Lines 4 – 11).

16. As per claim 25, Nessett teaches communicates over the first communication channel information for use in generating a shared secret, communicates the security value over the first communication channel, generates a first secret ostensibly shared with the device (Nessett, Col. 3 Lines 1 – 17) but fails to teach an interface to a first communication channel associated with a first communication method, an interface to a second communication channel associated with a communication method other than the first communication method and communicates over the second communication channel verification information related to the secret and enables the network to use the first secret upon receipt of an indication that a third party is assured that the first secret is shared with the device and detecting that the registration process has been initiated at the device by engaging a trigger coupled to the device.

However, in an analogous art Berman teaches an interface to a first communication channel associated with a first communication method, an interface to a second communication channel associated with a communication method other than the first communication method Berman, Paragraph 0062, another communication system used to verify information, communication between server and the

Art Unit: 2134

authenticating server, which in turn authenticates the user and the server) and Dujari teaches communicates over the second communication channel verification information related to the secret and enables the network to use the first secret upon receipt of an indication that a third party is assured that the first secret is shared with the device (Dujari, Col. 12 Lines 59 – 64) and Lintulampi teaches and detecting that the registration process has been initiated at the device by engaging a trigger coupled to the device (Lintulampi, Col. 1 Lines 66 – 67 and Col. 2 Lines 1 – 10, device registers with second device that connects to a network).

At the time the invention was made it would have been obvious to a person of ordinary skill in the art to use, Berman's mutual authentication with secure transport and client authentication with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of secure authentication (Berman, Paragraph 0008).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, Dujari's method of integrating third party authentication with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of being a secure form of authenticating information (Dujari, Col. 22 Lines 10 – 14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, Lintulampi's mobile communication system with Nessel's authenticated Diffie-Hellman key agreement protocol because it offers the advantage of providing services based on geographic locations (Lintulampi, Col. 1 Lines 4 – 11).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


Roderick Tolentino

Roderick Tolentino
Examiner
Art Unit 2134


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER